

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

TIMMINS SOFTWARE CORPORATION d/b/a  
MITREND

Plaintiff,

v.

EMC CORPORATION, DELL TECHNOLOGIES  
INC., and DELL INC.

Defendants.

C.A. No. 1:19-12053-IT

JURY TRIAL DEMANDED

**PROPOSED CONFIDENTIALITY STIPULATION AND PROTECTIVE ORDER**

**1. Proceedings and Form of Information Governed**

This Confidentiality Stipulation and Protective Order (the “Order” or “Protective Order”) shall govern any document, information, or other thing, including information in electronic form, furnished by any Party or non-party to any Party in connection with all phases of this action. The Parties acknowledge that they may request, and that the Court may direct, that, at trial, documents, information, or other things be handled other than as prescribed in this Order, and by stipulating to this Order neither Party waives the right to request such differential treatment. The form of information protected includes, but is not limited to, documents produced in the action, deposition testimony and exhibits and all copies of extracts, summaries, compilations, designations, and portions thereof, and responses to requests to produce documents or things, interrogatories, requests for admission, and non-party subpoenas.

**2. Definitions**

**A. Producing Party and Receiving Party**

The term “Party” refers to Plaintiff and Defendants in this action, including their respective counsel, retained experts, directors, officers, employees, business partners, or agents. The term “Producing Party” shall mean any Party to this action or any non-party, including its counsel, retained experts, directors, officers, employees, business partners, or agents, who produces any Protected Information (as defined herein). The term “Receiving Party” shall mean any Party to this action, including its counsel, retained experts, directors, officers, employees, business partners, or agents, who receives any Protected Information.

**B. Confidential Information**

The term “Confidential Information” shall mean any information, documents, material, or testimony produced for or disclosed in connection with this action to a Receiving Party, and designated by a Producing Party as CONFIDENTIAL, that the Producing Party believes, in good faith, constitutes, contains, reveals, relates to, or reflects information that: (i) the Producing Party would not normally reveal to third parties except in confidence, or has undertaken with others to maintain in confidence, (ii) is significantly sensitive, (iii) compromises confidential technical, sales, marketing, financial, or other commercially sensitive information, or (iv) is protected by a right to privacy under federal or state law or any other applicable privilege or right related to confidentiality or privacy.

The following information is not Confidential Information:

1. Any information that is or, after its disclosure to a Receiving Party, becomes part of the public domain as a result of publication not involving a violation of this Order or other obligation to maintain the confidentiality of such information;

2. Any information that the Receiving Party can show was already publicly known or made available prior to the disclosure; and
3. Any information that the Receiving Party can show by written records was received by it from a source who obtained the information lawfully and under no obligation of confidentiality to the Producing Party.

**C. Highly Confidential Information**

The term “Highly Confidential Information” shall mean any Confidential Information designated by the Producing Party as HIGHLY CONFIDENTIAL that the Producing Party believes, in good faith, constitutes, reveals, relates to, or reflects information that, if disclosed, would be highly likely to cause significant harm to an individual or to the business or competitive position of the Producing Party, including without limitation: (i) current or ongoing trade secrets and other extremely commercially sensitive marketing, financial, sales, research and development, or technical, data or information, (ii) current and ongoing commercially sensitive information, including, without limitation, information obtained from a non-party pursuant to a Non-Disclosure Agreement, (iii) commercially sensitive data relating to future products not yet commercially released and/or strategic plans, (iv) ongoing commercial agreements, settlement agreements, or settlement communications, or (v) commercially sensitive current or ongoing financial, technical, or strategic information. For the avoidance of doubt, this provision shall not preclude a Party from marking as HIGHLY CONFIDENTIAL historical information that fits within the foregoing categories, provided such historical information remains commercially sensitive.

**D. Highly Confidential – Source Code Information**

The term “Highly Confidential – Source Code Information” and “Source Code” shall mean information designated by the Producing Party as HIGHLY CONFIDENTIAL – SOURCE CODE that the Producing Party believes, in good faith, constitutes or comprises “Source Code,” meaning (i) computer source code, (ii) electronic information that is compiled into a product or platform, (iii) any documents containing such source code; or (iv) metadata about such source code, such as that contained in version control software. Metadata (such as information in version control software) about scripts (which are themselves not considered “Source Code”) may, but need not be, categorized as “Source Code.” Object code (which in general is not considered “Source Code”) may, but need not be, categorized as “Source Code” if the Producing Party believes in good faith that access to such object code may reveal sensitive details of or allow reverse engineering of underlying Source Code.

All scripts and/or Source Code shall be produced such that the Receiving Party is also able review all metadata associated such scripts and/or Source Code that is contained in any such version control system during their review of the scripts and/or Source Code. In addition, and if applicable, the scripts and/or Source Code shall be produced so that it can be reviewed as it is kept in the normal course of business in its native format, reviewable with developer’s tools and/or in the Producing Party’s independent development environment.

**E. Protected Information**

The term “Protected Information” shall mean and include, individually and collectively, documents, materials, and information designated by a Producing Party as “Confidential,” “Highly Confidential,” or “Highly Confidential – Source Code.”

### 3. **Presumptions as to Certain Material**

The following documents and things shall presumptively not be designated as HIGHLY CONFIDENTIAL or HIGHLY CONFIDENTIAL – SOURCE CODE: (a) scripts, instructions, procedures, or other information constituting, in whole or in part, Defendants’ Live Optics offering that are or were made available (including but not limited to “alpha,” “beta” or other such versions prior to “general availability” that were for testing, evaluation, or otherwise) to Defendants’ customers, partners, resellers, or distributors or otherwise made publicly available; (b) documents and things sent to or received from Defendants’ customers, partners, resellers, or distributors that concern TSC and/or its Mitrend® offering created on or prior to November 30, 2017; and (c) emails (and accompanying attachments) sent between or among Dell employees that reference TSC and/or its Mitrend® offering created on or prior to November 30, 2017; and (d) deposition testimony, discovery responses, or material regarding or constituting (a) - (c), above. A Party designating all or a portion of such material as HIGHLY CONFIDENTIAL or HIGHLY CONFIDENTIAL – SOURCE CODE shall, upon a challenge by the Receiving Party under Paragraph 13 or otherwise under this Order, be required to make showing that a CONFIDENTIAL designation is inadequate to protect the confidentiality of such material.

### 4. **Use of Protected Information**

Protected Information shall be used by the Receiving Party and approved persons to whom it is disclosed solely in the litigation or settlement of this action, or for use at trial and in any appellate proceeding in this action. Protected Information shall not be used by such Party or persons for any business or other purpose or disclosed to any person or entity not entitled under this Order to receive it, unless agreed to in writing by all parties to this action or as authorized by further order of the Court. All Protected Information shall be held in

confidence by each person to whom it is disclosed, and shall be carefully maintained so as to preclude access by persons who are not entitled to receive such information.

Except as may be otherwise ordered by the Court, any person may be examined as a witness at depositions and trial and may review with counsel in preparation for testimony and/or testify concerning all Protected Information of which such person has prior knowledge.

Without in any way limiting the generality of the foregoing:

- a) A present director, officer, agent, and/or employee of a Producing Party may be examined and may testify concerning all Protected Information of which the witness has personal knowledge;
- b) A former director, officer, agent, and/or employee of a Producing Party may be interviewed, examined and may testify concerning all Protected Information of which he or she has personal knowledge, including any Protected Information that refers to matters of which the witness has personal knowledge and which pertains to the period or periods of his or her employment; and
- c) Non-parties may be examined or testify concerning any document containing Protected Information of a Producing Party which appears on its face, from other documents or testimony, or the Receiving Party has a reasonable basis to believe to have been received from or communicated to the non-party as a result of any contact or relationship with the Producing Party or a representative of the Producing Party. Any person other than the witness, his or her attorney(s), or any person qualified to receive Protected Information under this Order shall be excluded from the portion of the examination concerning such information, unless the Producing Party consents to persons other than qualified recipients being present at the examination. If the witness is represented by an attorney

who is not qualified under this Order to receive such information, then prior to the examination, the attorney must provide a signed statement, in the form of Attachment A hereto, that he or she will comply with the terms of this Order and maintain the confidentiality of Protected Information disclosed during the course of the examination. In the event that such attorney declines to sign such a statement prior to the examination, the Parties, by their attorneys, shall jointly seek a protective order from the Court prohibiting the attorney from disclosing Protected Information and requiring compliance with this Protective Order.

Protected Information shall not be copied or otherwise produced by a Receiving Party, except for transmission to qualified recipients, without the written permission of the Producing Party, or, in the alternative, by further order of the Court. Nothing herein shall, however, restrict a qualified recipient from making working copies, abstracts, digests and analyses of Protected Information for use in connection with this litigation and such working copies, abstracts, digests and analyses shall be deemed Protected Information under the terms of this Order. Further, nothing herein shall restrict a qualified recipient from converting or translating Protected Information into machine readable form for incorporation into a data retrieval system used in connection with this action, provided that access to that Protected Information, in whatever form stored or reproduced, shall be limited to qualified recipients.

**5. Designation of Confidential Information and Highly Confidential Information for Protection Under This Order**

Any documents, information, materials, pleadings, expert statements or any other document produced or prepared in connection in this action that is reasonably and in good faith believed by the Producing Party to contain Confidential or Highly Confidential Information may be designated as "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL."



Such designation may be made by stamping or otherwise marking the material prior to production as follows: “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.”

In the case of written material, documents, or tangible items, the designation “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL” shall be made at or prior to the time the Receiving Party is provided a copy of the information. In lieu of marking the originals or documents, the Producing Party may mark the copies that are produced or exchanged. In producing original files and records for inspection, no marking need be made by the Producing Party in advance of the inspection. Any documents (including physical objects) made available for inspection by counsel for the Receiving Party prior to producing copies of selected items shall initially be considered, as a whole, to constitute Protected Information (unless otherwise designated at the time of inspection) and shall be subject to this Order. Thereafter, the Producing Party shall have a reasonable time, not to exceed ten (10) business days, to review and designate the appropriate documents as appropriate under the Order.

Where electronic files and documents are produced in native electronic format, such electronic files and documents shall be designated for protection under this Order by appending to the file names or designators information indicating whether the file contains Confidential or Highly Confidential Information, or shall use any other reasonable method for so designating material produced in electronic format.

If a Party produces or provides discovery of any Confidential or Highly Confidential Information without first labeling, marking, or designating it as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL,” then the Producing Party may thereafter give written notice promptly after discovery of such production or provision of discovery to the Receiving Party or Parties that the document, thing, transcript, or other embodiment of Confidential Information is



“CONFIDENTIAL” or “HIGHLY CONFIDENTIAL” and such Confidential Information should be treated in accordance with the provisions of this Order. The Receiving Party or Parties must treat such document, thing, transcript, or other embodiment of Confidential Information accordingly from the date such notice is received. Disclosure of such document, thing, transcript, or other embodiment of Confidential Information prior to receipt of such notice to persons not authorized to receive it shall not be deemed a violation of this Order or a waiver of the confidential status of the information; however, those persons to whom disclosure was made are to be advised that the material disclosed was “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL” and must be treated in accordance with this Order. The provisions of Paragraph 13 of this Order shall apply in the event of any disputes with respect to the propriety or correctness of a Party’s designation of the information as “CONFIDENTIAL” or “HIGHLY CONFIDENTIAL.”

6. **Designation of Highly Confidential – Source Code Information for Protection Under this Order**

Any documents, information, materials, pleadings, expert statements or any other tangible thing produced or prepared in connection in this action that is reasonably and in good faith believed by the Producing Party to contain or comprise Highly Confidential – Source Code Information may be designated as “HIGHLY CONFIDENTIAL – SOURCE CODE” and shall be made available for inspection and/or production pursuant to the following procedures and restrictions, unless otherwise agreed to by the Parties:

- a) The Producing Party may select one of two methods for producing Source Code.

First, Source Code in electronic format may be made available for inspection in native format on a standalone, password protected computer without Internet access or network access to other computers (the “Source Code Computer”) in a secure,

locked viewing room (the “Source Code Review Room”) at one of the following locations at the sole discretion of the Producing Party: (i) any office of the Producing Party’s outside counsel of record in Boston, Massachusetts; (ii) a single, third-party site located within the District of Massachusetts (Eastern Division) (*e.g.*, an escrow company), or (ii) if mutually agreed to, any other location. Second, alternatively, Source Code may be produced as it is kept in the normal course of business in its native format, in encrypted media and the Receiving Party shall copy the Source Code from the encrypted media to a standalone, non-networked Source Code Computer at the Receiving Party’s facility.

- b) Unless a Producing Party chooses to disclose Source Code prior to request from the Receiving Party, once the Source Code is ready for inspection, the Receiving Party shall provide ten (10) business days’ notice of its initial inspection Source Code. All other requests for inspection on future non-consecutive days shall made at least five (5) business days in advance of any such subsequent inspection. If the Receiving Party makes a written request for additional day(s) following a date initially requested, the Producing Party agrees to make reasonable efforts to accommodate such request. The Source Code Computer will be made available for inspection during regular business hours only, or otherwise agreed to by the Parties.
- c) A list of names of persons who will inspect the Source Code, and a list of requested date(s) and beginning and end times for inspecting the Source Code, will be provided to the Producing Party in conjunction with the written notice requesting inspection. The Receiving Party shall maintain a daily log of the names of persons who enter the Source Code Review Room to view the Source Code, and when they

enter and depart. Upon request, the Producing Party shall be entitled to a copy of such daily log. The Producing Party shall be entitled to have a person observe all entrances and exits from the Source Code Review Room.

- d) No recordable media, recordable devices, or input/output device, including, without limitation, sound recorders, computers, cellular telephones, peripheral equipment, floppy disks, cameras or any camera-enabled device, CDs, DVDs, or drives of any kind, shall be permitted into the Source Code Review Room. The Producing Party shall make accommodation to secure any such media and devices brought by anyone reviewing Source Code during the period of such review.
- e) The Receiving Party's outside counsel and/or experts may request that software tools for viewing and searching Source Code and/or other electronic files be made available for installation or use on the Source Code Computer. The Receiving Party may provide the Producing Party with a CD, DVD, or USB memory stick containing software tools that are to be installed or made available on a Source Code Computer. The Producing Party shall have the right to review and further confer regarding such software tools prior to those tools being installed or made available on a Source Code Computer. The Producing Party will provide reasonable accommodations to the extent that administrative privileges are required for installation or use of such software tools.
- f) Under no circumstances is Source Code to be copied, printed, or transmitted in electronic form without the prior authorization of the Producing Party. The Producing Party may enforce reasonable restrictions on the review of Source Code in electronic format, including making Source Code available on a stand-alone, non-

networked computer, with input/output connections disabled such that Source Code cannot be removed, copied, or otherwise transferred from the Source Code Computer and the Source Code Computer cannot be connected to the internet.

- g) The Receiving Party's outside counsel, expert(s), and/or consultant(s) may take handwritten notes relating to the Source Code, but may not copy the Source Code into the notes and may not take such notes electronically. The notes must be marked "HIGHLY CONFIDENTIAL – SOURCE CODE." The Receiving Party's outside counsel, expert(s), and/or consultants' notes are to be used in conjunction with this action only and for no other purpose and are to be destroyed within ten (10) days of the final resolution of this case. No other written or electronic record of the Source Code is permitted except as otherwise provided herein.
- h) The Producing Party may visually monitor the activities of the Receiving Party's representatives during any Source Code review, but only to ensure compliance with the security procedures enumerated herein. Any observer used by the Producing Party shall be a reasonable distance away from the Receiving Party's representatives during the Source Code review so as to refrain from overhearing a whispered conversation (in order that the Receiving Party's representatives can quietly discuss the Source Code in the course of their review). If the door to the Source Code Review Room is not glass and/or the Source Code Room is not otherwise observable from outside, the door shall remain open at all times during the review.
- i) Unless otherwise agreed in advance by the Parties in writing, following each inspection, the Receiving Party's outside counsel, expert(s), and/or consultant(s) shall remove all physical notes, documents, and other materials from the room that

may contain work product and/or attorney-client privileged information. The Producing Party shall not be responsible for any items left in the Source Code Review Room after an inspection session.

- j) Unless otherwise permitted herein, no copies of all or any portion of the Source Code may leave the Source Code Review Room. Further, no other written or electronic record of the Source Code is permitted. The Receiving Party will not print, copy, remove, or otherwise transfer any Source Code from the Source Code Computer including, without limitation, copying, removing, or transferring the Source Code onto any recordable media or recordable device.
- k) A Party shall be entitled to have printed, in paper form, portions of the Source Code in blocks of not more than ten (10) consecutive pages, or an aggregate total of not more than 250 pages, for use by the Receiving Party's outside counsel and outside experts or consultants as part of case preparation activity; provided that all such paper forms shall be on goldenrod colored paper labeled on each page with a legend designating them as "HIGHLY CONFIDENTIAL – SOURCE CODE," together with a unique number for each page. The printed pages shall constitute part of the Source Code produced by the Producing Party in this action. A copy of printed pages shall be transmitted to the Receiving Party within five (5) business days of the printing, or such additional time as necessary due to the volume requested. The entire code shall not be printed. The printed pages shall be bates numbered and the lines of code thereon shall be numbered by line number for reference in other documents. If a Receiving Party requests Source Code beyond the limits set forth in this paragraph, and if the Parties cannot reach agreement on increasing the number

of pages to be printed beyond those limits, then the Receiving Party may seek relief from the Court for the production of such additional materials.

- l) If the Producing Party objects that the requested printed portions are not reasonably necessary to any case preparation activity, the Producing Party shall make such objection known to the Receiving Party within five (5) business days. If after meeting and conferring the Producing Party and the Receiving Party cannot resolve the objection (where such meet-and-confer need not take place in person), the Receiving Party may seek a Court resolution of whether the printed Source Code in question is reasonably necessary to any case preparation activity. Contested Source Code print outs need not be produced to the Requesting Party until the matter is resolved by the Court.
- m) The Receiving Party's outside counsel of record and any person receiving a copy of any Source Code shall maintain and store any copies of the Source Code at their offices in a manner that prevents duplication of or unauthorized access to the Source Code, including, without limitation, storing the Source Code in a locked room or cabinet at all times when it is not in use. The Receiving Party's outside counsel of record and any person receiving a copy of any Source Code shall maintain a log of the identity of any person that accesses the room where Source Code is kept, along with the time and date of any such access. Upon a showing of good cause by the Producing Party, such log shall, upon notice of three (3) business days, be made available to the Producing Party. The Producing Party shall, however, be entitled to the names of the persons on said log upon request, without the need to show good cause.

- n) The Receiving Party's outside counsel shall maintain a log of all copies of the printed pages of Source Code (received from a Producing Party) that are delivered by the Receiving Party to any qualified person as described herein (other than the Receiving Party's outside counsel of record). The log shall include the names of the recipients and reviewers of copies and locations where the copies are stored. Upon a showing of good cause by the Producing Party, the Receiving Party shall provide reasonable assurances and/or descriptions of the security measures employed by the Receiving Party and/or qualified person that receives a copy of any portion of the Source Code.
- o) For depositions, copies of Source Code that are marked as deposition exhibits shall not be provided to the Court Reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers. All paper copies of Source Code brought to the deposition shall be destroyed or returned to a locked room or cabinet where the Receiving Party keeps Source Code in a timely manner following the deposition.
- p) Any printed pages of Source Code may not be copied, digitally imaged or otherwise duplicated, except in limited excerpts necessary to attach as written responses to interrogatories, deposition preparation materials for use by outside counsel, exhibits to expert reports or court filings designated "HIGHLY CONFIDENTIAL – SOURCE CODE."
- q) Except as provided in this paragraph, the Receiving Party may not create an electronic copy or image of the Source Code from the paper copy (e.g., may not scan the source code to a PDF, or photograph the code). The Receiving Party may



create an electronic copy or image of limited excerpts of the printed pages of Source Code only to the extent necessary in a written response to an interrogatory, pleading, exhibit, expert report, discovery document, deposition transcript, other Court document, or any drafts of these documents (“Source Code Documents”). All electronic copies must be labeled “HIGHLY CONFIDENTIAL—SOURCE CODE.” The Receiving Party shall only include such excerpts as are reasonably necessary for the purposes for which such part of the Source Code is used.

Electronic copies or images of Source Code shall not be included in correspondence between the Parties (references to production numbers shall be used instead) and shall be omitted from pleadings and other papers except to the extent permitted herein. The electronic file containing such excerpts shall be encrypted using commercially reasonable encryption software including password protection. The communication and/or disclosure of electronic files containing any portion of Source Code shall at all times be limited to individuals who are authorized to see Source Code under the provisions of this Protective Order. The Receiving Party shall include in the logs maintained pursuant to Paragraphs 6(m) and 6(n) a record of all electronic copies of Source Code in the possession of its retained consultants, including the names of such recipients and reviewers of any electronic or paper copies and the locations where the copies are stored.

- r) To the extent portions of Source Code are quoted in a Source Code Document, either (1) the entire document will be stamped and treated as HIGHLY CONFIDENTIAL—SOURCE CODE or (2) those pages containing quoted Source

Code will be separately bound, and stamped and treated as HIGHLY  
CONFIDENTIAL—SOURCE CODE.

- s) All copies of any portion of the Source Code in whatever form shall be, at the option of the Producing Party, either returned to the Producing Party or destroyed if they are no longer in use.
- t) The provisions of Paragraph 13 of this Order shall apply in the event of any disputes with respect to the propriety or correctness of a Party's designation of the information as "HIGHLY CONFIDENTIAL – SOURCE CODE."
- u) For the sake of clarity, the above provisions regarding the use and disclosure of Source Code shall supersede any other rules regarding Source Code, including any standard default rules.

**7. Disclosure of "CONFIDENTIAL" Materials**

All documents, information, or other things designated "CONFIDENTIAL" may be disclosed by the Receiving Party to and only to:

- a) The outside and in-house litigation counsel of record in this action and their respective partners, associates, clerks, legal assistants, and support personnel, and further including independent organizations and employees thereof retained by such attorneys to provide professional litigation support services in this action, such as translation, graphics, design, and document processing;
- b) Court personnel, court reporters, and videographers involved in this action;
- c) Independent experts and consultants retained in this action, and the employees of such experts and consultants who are assisting them, who have been furnished with

a copy of this Order and have executed a declaration in the form attached hereto as Exhibit A, a copy of which shall be retained by counsel;

- d) Up to three (3) employees of each Receiving Party who are director level or above team members with responsibility for overseeing this litigation, and who have signed the form attached hereto as Attachment A (which must be retained by the Receiving Party but, unless good cause is shown, need not be provided to the Producing Party);
- e) Jury or trial consulting service providers, including mock jurors (who may not receive or retain physical copies of any Protected Information), who have been furnished with a copy of this Order and have executed a declaration in the form attached hereto as Exhibit A, a copy of which shall be retained by counsel;
- f) Such other persons as hereafter may be designated by written agreement of Parties in this action or by order of the Court, such order obtained on noticed motion (or on shortened time as the Court may allow) permitting such disclosure; and
- g) The author or recipient of the Protected Information or any deposition witness who is appearing on behalf of the Party that produced the Protected Information.

**8. Disclosure of “HIGHLY CONFIDENTIAL” Materials**

All documents, information, or other things designated “HIGHLY CONFIDENTIAL” are included within the meaning of Highly Confidential Information as used in this Order, and all the provisions set forth in this Order that apply to Protected Information also apply to material designated “HIGHLY CONFIDENTIAL.” Notwithstanding any other provision of this agreement, however, access to documents, information, and other things designated “HIGHLY

CONFIDENTIAL” shall be limited to persons referred to in subparagraphs 7(a), (b), (c), (e), (f), and (g) above.

**9. Disclosure of “HIGHLY CONFIDENTIAL – SOURCE CODE” Materials**

All documents, information, or other things designated “HIGHLY CONFIDENTIAL – SOURCE CODE” are included within the meaning of Highly Confidential – Source Code Information as used in this Order, and all the provisions set forth in this Order that apply to Highly Confidential Information also apply to material designated “HIGHLY CONFIDENTIAL – SOURCE CODE.” Notwithstanding any other provision of this agreement, only the following individuals shall have access to “RESTRICTED CONFIDENTIAL—SOURCE CODE” materials, absent the express written consent of the Producing Party or further court order:

- a) Outside counsel of record for the parties to this action, including any attorneys, paralegals, technology specialists and clerical employees of their respective law firms;
- b) Up to three (3) outside technical advisors or experts per Party, pre-approved in accordance with Paragraphs 10(A) through (F) of this Order and identified as having reviewed Source Code;
- c) The Court, its technical advisor (if one is appointed), the jury, court personnel, and court reporters or videographers recording testimony or other proceedings in this action. Court reporters and/or videographers shall not retain or be given copies of any portions of the Source Code. If used during a deposition, the deposition record will identify the exhibit by its production numbers; and

- d) While testifying at deposition or trial in this action only: (i) any current or former officer, director or employee of the Producing Party or original source of the information; (ii) any person designated by the Producing Party to provide testimony pursuant to Rule 30(b)(6) of the Federal Rules of Civil Procedure; and/or (iii) any person who authored, previously received (other than in connection with this litigation), or was directly involved in creating, modifying, or editing the Source Code, as evident from its face, from the associated metadata, or reasonably certain in view of other testimony or evidence. Persons authorized to view Source Code pursuant to this sub-paragraph shall not retain or be given copies of the Source Code except while so testifying.

**10. Disclosure of Technical Advisers and Experts**

A. Information designated by the Producing Party under any category of HIGHLY CONFIDENTIAL – SOURCE CODE materials and such copies of this information as are reasonably necessary for maintaining, defending or evaluating this litigation may be furnished and disclosed to the Receiving Party’s technical advisers or experts (both referred to herein as “technical advisers”), and their necessary support personnel as further provided herein.

B. No disclosure of HIGHLY CONFIDENTIAL – SOURCE CODE materials to a technical adviser or their necessary support personnel shall occur until the technical advisor has signed the form attached hereto as Attachment A, and a signed copy has been provided to the Producing Party; and to the extent there has been an objection under Paragraph 13 of this Order, that objection is resolved according to the procedures set forth below.

C. A Party desiring to disclose HIGHLY CONFIDENTIAL – SOURCE CODE materials to a technical adviser for the first time shall also give prior written notice of the

intended disclosure by email to all counsel of record in the litigation, and the Producing Party shall have ten (10) business days after such notice is given to object in writing to the disclosure. The Party desiring to disclose HIGHLY CONFIDENTIAL – SOURCE CODE materials to a technical adviser must provide the following information for each technical adviser: name, address, curriculum vitae, current employer, employment history, a list of every entity for which the technical adviser has consulted or is currently consulting in the field of IT infrastructure analysis within the past four (4) years, and a listing of cases in which the technical adviser has testified as an expert at trial or by deposition within the past four (4) years. Notwithstanding the preceding sentence, the Party receiving such disclosure may, upon a showing of good cause with respect to each such proposed technical adviser, seek information for up to four (4) additional prior years (for a total of eight (8)) from the Party seeking to disclose the HIGHLY CONFIDENTIAL – SOURCE CODE materials to such technical adviser. No HIGHLY CONFIDENTIAL – SOURCE CODE materials shall be disclosed to such technical adviser until after the expiration of the foregoing notice period and resolution of any objection. Subsequent disclosure of HIGHLY CONFIDENTIAL – SOURCE CODE materials to the technical adviser shall not require any additional notice, and such technical adviser shall be entitled to review all HIGHLY CONFIDENTIAL – SOURCE CODE materials in accordance with the terms of this Order. If the technical expert reviews Source Code of the Opposing Party in accordance with the provisions of this Order, he or she shall be identified to the Producing Party to ensure compliance with Paragraph 9(b).

D. A Party objecting to disclosure of HIGHLY CONFIDENTIAL – SOURCE CODE materials to a technical adviser shall state with particularity the ground(s) of the objection. The objecting Party's consent to the disclosure of HIGHLY CONFIDENTIAL –

SOURCE CODE materials to a technical adviser shall not be unreasonably withheld, and its objection must be based on that Party's good faith belief that disclosure of its HIGHLY CONFIDENTIAL – SOURCE CODE materials to the technical adviser will result in specific business or economic harm to that Party, or that it would be otherwise inappropriate for the technical advisor to receive its HIGHLY CONFIDENTIAL – SOURCE CODE materials.

E. If after consideration of the objection, the Party desiring to disclose the HIGHLY CONFIDENTIAL – SOURCE CODE materials to a technical adviser refuses to withdraw the technical adviser, then that Party shall provide notice to the objecting Party. Thereafter, the objecting Party shall move the Court, within five (5) business days of receiving such notice, for a ruling on its objection. A failure to file a motion within the five (5) business day period, absent an agreement of the Parties to the contrary or for an extension of such five (5) business day period, shall operate as an approval of disclosure of HIGHLY CONFIDENTIAL – SOURCE CODE materials to the technical adviser. The Parties agree to cooperate in good faith to shorten the time frames set forth in this paragraph if necessary to abide by any discovery or briefing schedules.

F. The objecting Party shall have the burden of showing to the Court “good cause” for preventing the disclosure of its HIGHLY CONFIDENTIAL – SOURCE CODE materials to the technical adviser.

#### **11. Court Procedures**

Counsel for the Parties shall follow all applicable Local Rules, including Local Rule 7.2 regarding motions for impounding confidential materials, and customs for the Court when filing Protected Information under seal. In particular, the Party seeking or requesting that the information be filed under seal shall establish the requisite “good cause,” namely other than the



fact that the Parties agree as to confidentiality or that the documents were exchanged pursuant to this Protective Order.

No Party shall file any Protected Information with the Court until the Court determines whether such material may be filed under seal or on the public docket. A Party seeking to include such material in a filing shall timely file redacted version of the filing on the public docket and shall contemporaneously serve an unredacted version of the filing on counsel for all Parties. To the extent the filing contains the Protected Information of a non-party, the filing Party shall within one (1) business day of filing provide notice to the non-party of the non-party's Protected Information contained within the filing.

Within five (5) business days of service of the unredacted version of the filing, or for non-parties within five (5) business days of notice by the filing Party, any Party or non-party seeking to maintain the confidentiality of any Protected Information in the filing shall file a Motion to Impound Designated Material in accordance with the District of Massachusetts Local Rule 7.2 and ECF Administrative Procedures. The Motion to Impound shall reference this Order, describing the general nature and purpose for submitting the paper (i.e. exhibit to declaration in support of motion, etc.), and explain the good cause to support the request for leave to file the document under seal. Reference to a document's designation as Protected Information pursuant to the Protective Order, without more, will not suffice to show a particularized need for impoundment.

If the Court grants leave to file any of the Protected Information in the filing under seal, the filing Party shall refile the filing under seal in an unredacted form, placing the legend "FILED UNDER SEAL PURSUANT TO PROTECTIVE ORDER" above the caption and conspicuously on each page of the filing. Exhibits to a filing shall conform to the labeling

requirements set forth in this Order. If the Court denies a Motion to Impound, or if a Party declines to file a Motion to Impound, for any information redacted from the original filing, the filing Party shall refile the filing on the public docket with the relevant portions of the filing unredacted. The filing Party shall complete these additional filings within five (5) business days of the Court's ruling on the last motion to impound, or in the event no Party files a Motion to Impound, the filing Party shall refile the filing on the public docket in an unredacted form within five (5) business days of the last day to file a Motion to Impound.

Outside attorneys of record for the Parties are hereby authorized to be the persons who may retrieve confidential exhibits and/or other confidential matters filed with the Court upon termination of this litigation without further order of this Court. No material or copies thereof so filed shall be released except by order of the Court. Notwithstanding the foregoing and with regard to material designated as "HIGHLY CONFIDENTIAL—SOURCE CODE," the provisions of Paragraphs 2(D) and 9 are controlling to the extent those provisions differ from this paragraph.

Nothing herein shall be construed to affect in any manner the admissibility at trial of any document, testimony, or other evidence.

**12. Party's Own Information**

The restrictions on the use of Protected Information established by this Order are applicable only to the use of Protected Information received by a Party from another Party or from a non-party in connection with this action. A Party is free to do as it wishes with its own information, but in the event a Party possesses Protected Information of another pursuant to a written confidentiality agreement, the Party requesting such information shall not be entitled

to discover such information without the consent of the other Party or upon further order of the Court.

**13. Contesting a Designation**

The Parties shall use reasonable care when designating documents or information as Protected Information. A Party may seek the removal of the “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL,” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” designations from particular items. In such event, the following procedure shall apply:

- a) A Receiving Party may at any time request that the Producing Party remove or modify the Protected Information designation with respect to any document or information contained therein. A Party shall not be obligated to challenge the propriety of a designation of any category of Protected Information at the time of production, and a failure to do so shall not preclude a subsequent challenge thereto.
- b) The Party or person seeking such removal shall give counsel of record for the Party asserting the protection written notice thereof, supported by the reason therefor specifying the document, information, or other thing as to which such removal is sought.
- c) The Parties shall use reasonable efforts to resolve promptly and informally such disputes. If the Parties cannot reach agreement concerning the matter within seven (7) business days after service of the notice, or such shorter time as the Court may allow, then the Party seeking the removal of the “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL,” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” designations may seek informal resolution with the Court or file and serve a motion for appropriate relief. The parties agree that they will take reasonable steps to fully

brief and present the motion to the Court in the most expeditious fashion reasonably possible under the circumstances.

- d) The party seeking to designate the information and/or document as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” has the burden, in response to any such motion, to establish the appropriateness of the protection sought.
- e) Until a determination by the Court, the information subject to a designation challenge shall be treated as having been properly designated and subject to the terms of this Order.

#### **14. Depositions**

Information and testimony that is: (a) disclosed or elicited at the deposition of a party or one of its present or former officers, directors, employees, agents, or independent experts retained by a party for purposes of this litigation, and/or (b) protected by a contractual or statutory confidentiality provision (regardless of the identity of the deponent), may be designated as Protected Information by indicating on the record at the deposition that the testimony contains information designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL,” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” and subject to the provisions of this Order. A Party may also designate information disclosed at such deposition as Protected Information by notifying all Parties, in writing, of the specific pages and lines of the transcript that contain Protected Information, and the level of designation of such information. Unless otherwise designated before, all depositions shall be treated as “HIGHLY CONFIDENTIAL” for a period of twenty-one (21) calendar days after a full and complete transcript of said deposition is available. After this twenty-one (21) day period and unless

otherwise designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL,” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” the deposition transcript shall not be treated as containing Protected Information.

Whenever any documents, information, or other things designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” are to be discussed or disclosed in a deposition, any Party claiming such confidentiality may exclude from the room any person who is not entitled to receive documents, information, or other things designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE.”

#### **15. Subpoenas**

In the event any person or Party having possession, custody, or control of any Protected Information receives a subpoena, or other process or order to produce such information, such person or Party shall, within five (5) business days, or no later than twenty-four (24) hours before the time for compliance if the time for compliance is shorter than five (5) business days, notify in writing the attorneys of record of the Party claiming such confidential treatment of the item, document, or information sought by such subpoena, process, or order; shall furnish those attorneys of record with a copy of said subpoena, process, or order; and shall provide reasonable cooperation with respect to any procedure to protect such information or matter as may be sought to be pursued by the Party whose interests may be affected. If the Party asserting confidentiality makes a motion to quash or modify the subpoena, process, or order, there shall be no disclosure of the subject matter objected to pursuant to the subpoena, process, or order until the Court has ruled upon the motion, and then only in accordance with the Court’s ruling. If no such motion is made by the Party asserting confidentiality despite a reasonable opportunity to do so, the

person or Party receiving the subpoena, process, or order shall be entitled to comply with it, provided it has fulfilled its obligations pursuant to this Order.

**16. No Waiver**

Other than as specified herein, neither the taking of nor the failure to take any action to enforce the provisions of this Order, nor the failure to object to any designation or any such action or omission, shall constitute a waiver of any right to seek and obtain protection or relief in this action or any other action including, but not limited to, the right to claim that any information is or is not proprietary to any Party, is or is not entitled to particular protection, or that such information does or does not embody Protected Information of any Party. The procedures set forth herein shall not affect the rights of the Parties to object to discovery on grounds other than those related to confidentiality, nor shall it relieve a Party of the necessity of proper response to discovery devices.

**17. Return of Information**

Within sixty (60) calendar days after the conclusion of this action, whether by judgment and exhaustion of all appeal rights, or by settlement, all Protected Information and all documents that reflect such information shall be, at the option of the Receiving Party, (i) delivered to the Party that furnished such Protected Information, or (ii) in lieu of delivery to the Producing Party, destroyed, in which event counsel shall give written notice of such destruction to opposing counsel. The attorneys of record shall ensure that all the Protected Information in the possession, custody, or control of their experts and consultants is also destroyed or returned to the Party that furnished such Protected Information, for return to the Producing Party or destruction by the Receiving Party. In no event shall a Party, its experts, or consultants retain a copy of Protected Information produced to it, although they may retain a copy of any final

expert report in accordance with the restrictions of this Order. Notwithstanding the foregoing, counsel of record in this action may retain: (1) one copy of all pleadings, motions, and briefs (including supporting or opposing memoranda and exhibits), filed with the Court and/or served upon or by opposing counsel; (2) one copy of each transcript of any depositions (and summaries thereof) taken in this action, including all exhibits thereto; (3) all documents or other materials marked as hearing or trial exhibits; and (4) all notes, summaries, descriptions, abstracts, or other work product materials prepared in anticipation of or for use in the present action; provided, however that access to Protected Information contained in any of the materials identified in subparagraphs (1) through (4), above, shall be limited to counsel of record for their own internal use, and that such information shall not be provided to any non-party without the express prior written permission of counsel of record for the opposing Party or pursuant to court order.

**18. Non-Parties**

At the request of a non-party who produces documents or testimony in the case, and who is willing to be bound by the terms of this Order, the terms of this Order will be applied to protect the confidentiality of any documents or information supplied by that non-party in the course of this litigation so long as such non-party designates the documents or information as Protected Information consistent with the terms of this Order. A non-party's use of this Protective Order to protect its Protected Information does not entitle that non-party access to the Protected Information produced by any Party or any other non-party in this case.



**19. Court's Jurisdiction**

The Court retains jurisdiction to make such amendments, modifications, deletions, and additions to this Order as the Court may from time to time deem appropriate. The provisions of this Order regarding the use and/or disclosure of Protected Information shall survive the termination of this action, and the Court shall retain jurisdiction with respect to this Order.

**20. Privilege**

**A. Logs**

Consistent with the Federal Rules of Civil Procedure, a Party withholding or redacting any responsive document on the grounds of privilege, immunity, or any similar claim shall provide to the Receiving Party a privilege log, except that the Parties shall have no obligation to log: (a) information generated on or after October 3, 2019 (*i.e.*, date the Complaint was filed); and (b) activities undertaken in compliance with the duty to preserve information (including, but not limited to, litigation hold letters) are protected from disclosure under Fed. R. Civ. P. 26(b)(3)(A) and (B) and need not be included in the privilege log.

For each document withheld or redacted, the privilege log shall contain the following information: (i) the date of the document; (ii) the identity of all persons who authored, signed, or otherwise prepared the document; (iii) the identity of all persons designated as addressees or copyees; (iv) a description of the contents of the document that, without revealing information itself privileged or protected, is sufficient to understand the subject matter of the document and the basis of the claim of privileged or immunity; (v) the type or nature of the privilege asserted (e.g., attorney-client privilege, work product doctrine, etc.); and (vi) for redacted documents only, the Bates numbers corresponding to the first and last page of any document redacted. For all individuals listed on a log whose role as an attorney is the basis for a claim of privilege, the

privilege log shall contain some indication that the individual is an attorney (for example, an asterisk next to each attorney's name).

Privilege logs will identify e-mail chains as a single entry and note that they are chains, as long as all persons participating in the chains are identified.

When a Party redacts information that is protected by the attorney-client privilege or work product protection ("Privileged Information"), that redaction will be labeled "Redacted – Privilege."

**B. Clawbacks**

This Order protects any disclosure of Privileged Information, whether that disclosure is inadvertent or otherwise and is entered pursuant to Rule 502(d) of the Federal Rules of Evidence.

Subject to the provisions of this Order, if the Producing Party discloses information in connection with this action that the Producing Party thereafter claims to be Privileged Information, the disclosure of that Privileged Information will not constitute or be deemed a waiver or forfeiture—in this action or any other action—of any claim of privilege or work product protection that the Producing Party would otherwise be entitled to assert with respect to the Privileged Information and its subject matter.

Each Party is entitled to decide, in its sole discretion, the appropriate degree of care to exercise in reviewing materials for privilege. Irrespective of the care that is actually exercised in reviewing materials for privilege, the Court hereby orders that disclosure of Privileged Information in discovery conducted in this Action shall not waive any claim of privilege or work product protection that the Producing Party would otherwise be entitled to assert with respect to the Privileged Information and its subject matter.

A Producing Party must notify the party receiving the Privileged Information, in writing, that it has disclosed that Privileged Information without intending a waiver by the disclosure following in the procedure in Paragraph 20(D). Upon receipt of notification, the Receiving Party shall (a) destroy or return all copies, electronic or otherwise, of such document or other information; (b) not use or disclose the document or information until the claim of privilege or work product protection is resolved; and (c) shall provide a certification that it has—to the best of its knowledge—destroyed or returned all copies of such document or other information and will cease further review, dissemination, and use of the Privileged Information following the procedure in Paragraph 20(D).

The Receiving Party has an obligation to notify the Producing Party when it, in good faith, believes that any documents, materials, or information produced by the Producing Party may constitute Privileged Information and allow the Producing Party to evaluate whether such document, material, or information should be subject to a Clawback under the provisions of this Order.

This Order shall be interpreted to provide the maximum protection allowed to the Producing Party by Federal Rule of Evidence 502(d). However, if for any reason a Court finds that this Paragraph 20(B) is inapplicable to Privileged Information, then Rule 502(b) will apply in its absence.

**C. Challenges to Clawbacks**

Nothing in this Order shall limit the Receiving Party's right to challenge (on grounds unrelated to the fact or circumstances of the disclosure) the Producing Party's claim that Privileged Information is protected from disclosure by the attorney-client privilege or work product doctrine. The Parties agree to use the procedure in Paragraph 20(D) for any such

challenges. If, after undertaking an appropriate meet-and-confer process, the Parties are unable to resolve any dispute they have concerning the protection of documents for which a claim of privilege has been asserted, the Receiving Party may file the appropriate motion or application as provided by the Court's procedures to compel production of such material. Any Privileged Information submitted to the Court in connection with a challenge to the Producing Party's claim of attorney-client privilege or work product protection shall not be filed in the public record, but rather shall be redacted, filed under seal, or submitted for *in camera* review.

**D. Disclosure of Privileged Information**

Notwithstanding anything to the contrary in Rule 26(b)(5)(A) and (B) of the Federal Rules of Civil Procedure, the production or disclosure of any document or tangible thing (including information) that should have been withheld subject to a claim of attorney-client privilege or work product immunity, or other privilege or immunity, shall in no way prejudice or otherwise constitute a waiver of, or estoppel as to, any claims of privilege or work product immunity. In such an event, the Producing Party shall send to each Receiving Party a written request for return of the produced or disclosed document or thing promptly after becoming aware of such production. Within five (5) business days of receiving a written request to do so from the Producing Party, the Receiving Party shall: (a) return to the Producing Party any documents or tangible items that the Producing Party represents are covered by a claim of attorney-client privilege or work-product immunity, or other privilege or immunity, and were inadvertently or mistakenly produced; (b) destroy any extra copies or summaries of, or notes relating to, any such produced information, including any electronic records thereof; and (c) shall provide a certification that it has—to the best of its knowledge—destroyed or returned all copies of such document or other information and will cease further review, dissemination, and use of the

Privileged Information. The Receiving Party shall not utilize the information contained in the produced documents or things for any purpose, or disseminate or transmit such information.

If the Receiving Party wishes to contest that any such document or thing is protected from disclosure by the attorney-client privilege, work product immunity or other privilege or immunity from discovery, it shall so notify the Producing Party in writing when the document or thing is returned to the Producing Party ("Notice of Designation").

Within five (5) business days after receiving a Notice of Designation, the Producing Party shall provide to the Receiving Party for each document or thing a description of the basis for the claim of privilege or immunity.

Within five (5) business days after receiving such description, the Receiving Party may seek relief from the Court to compel production of such documents and things, the protection of which is still disputed, in accordance with the procedures set forth in Local Rule 37.1 for resolution of discovery disputes. The Party claiming the privilege or immunity shall have the burden of proving that such privilege or immunity exists.

With respect to documents and things subsequently generated by a Receiving Party, which documents and things contain information derived from such inadvertently produced documents and things, if the Receiving Party does not notify the Producing Party that the Receiving Party disputes the claims of attorney-client privilege or work-product immunity, or if the Court rejects any challenge by the Receiving Party to the privileged status of the inadvertent production, the Receiving Party shall either destroy the derivative documents and things or redact from them all such derivative privilege or work-product information in a manner such that the derivative information cannot in any way be retrieved or reproduced.

If, in a deposition, hearing, or other proceeding, the Party who made the production or disclosure makes a request on the record for return of the produced or disclosed document or thing within a reasonably prompt period of time after recognizing that the information has been produced or disclosed, all copies of the produced or disclosed document or thing present at the deposition, hearing, or other proceeding shall immediately be sequestered and there shall be no further use of the produced or disclosed document or thing. For the avoidance of any dispute, the marking of an produced or disclosed document or thing as an exhibit at deposition, hearing, or other proceeding has no bearing on the timeliness of the request for return.

The procedures set forth in this Paragraph 20(D) for challenging the privileged status of a production shall not result in any waiver of the attorney-client privilege, the work product immunity, or any other privilege or immunity.

**21. Prosecution Bar**

Absent written consent from the Producing Party, any individual who substantively reviews information designated “HIGHLY CONFIDENTIAL” or “HIGHLY CONFIDENTIAL—SOURCE CODE” (a “Patent Prosecution Restricted Person”) shall not be involved in the prosecution of patents or patent applications in the field of computer software that is designed and intended for the collection of computer files in a business’ IT infrastructure that contain information about the configuration, capacity, and performance of servers, storage, and backup, as well as the analysis of such information, in any foreign or domestic agency, including the United States Patent and Trademark Office. For purposes of this paragraph, “Prosecution” means directly or indirectly drafting, amending, or advising on the scope or maintenance of patent claims. Prosecution includes, for example, original prosecution, reissue, reexamination, and any other post-grant proceedings that may affect the scope of the claims of a

patent or patent application. Prosecution does not include representing a party challenging a patent before a domestic or foreign agency (including, but not limited to, a reissue protest, ex parte reexamination, inter partes reexamination, post-grant review, inter partes review, or covered business method patent review). This paragraph shall apply beginning on the date the individual receives access to information designated “HIGHLY CONFIDENTIAL” or “HIGHLY CONFIDENTIAL—SOURCE CODE,” and shall continue until three years after the date on which the person first receives access to the information. If a Patent Prosecution Restricted Person breaches the restrictions set forth in this paragraph, the patent family that was the subject of Prosecution shall not be enforceable against the Producing Party and any of its current or future affiliates or subsidiaries. Without limiting any Party’s remedies for violations of other provisions of this Protective Order, the foregoing sentence states the sole remedy for violation of this paragraph.

**22. No Limitation of Other Rights**

This Order shall be without prejudice to the right of any Party to oppose production of any information on any and all grounds other than confidentiality.

**23. Release From or Modification of This Order**

This Order is entered without prejudice to the right of any Party to apply to the Court at any time for additional protection, or to release, rescind, or modify the restrictions of this Order, to determine whether a particular person shall be entitled to receive any particular information or to seek relief from disclosure of privileged or work-product information. This Order does not preclude all of the Parties to this Order from entering into any stipulation (in writing or on the record) constituting a modification of this Order. On any motion seeking disclosures beyond



those authorized by this Order, the burden will be on the Receiving Party to justify the disclosure.

**24. No Contract**

To the extent that the Parties have agreed on the terms of this Order, such stipulation is for the Court's consideration and approval as an Order. The Parties' stipulation shall not be construed to create a contract between the Parties or between the Parties and their respective counsel.

**25. Effective Date**

Documents that have been produced in this case on and have been designated as Protected Information prior to the entry of this Order shall henceforth be subject this Order.

**26. Miscellaneous Provisions**

A. Any of the notice requirements herein may be waived, in whole or in part, but only in writing signed by outside counsel of record for the Party against whom such waiver will be effective.

B. With respect to any summaries of financial information provided by the Producing Party, the Receiving Party shall password protect any such summaries or information from those summaries that are in a digital format or converted into a digital format (e.g., PDF, TIFF, Word, Excel). Any financial summaries transmitted from or to authorized recipients outside of the Receiving Party's outside counsel's office shall be by hand, through a secure transport carrier (e.g., Federal Express), on encrypted media, or encrypted file transfer.

C. The Receiving Party shall have and maintain appropriate physical, organizational, and technical processes, security standards, and procedures to protect against a data breach ("Appropriate Safeguards"), and shall ensure that its professional vendors, technical advisors,

and any other person or entity that receives Protected Information under this Protective Order implements and maintains such Appropriate Safeguards. For purposes of this paragraph, a data breach shall include but is not limited to any accidental, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, use, modification, disposal, compromise, or access to Protected Information or any act or omission that compromises or undermines the physical, technical, or organizational safeguards put in place by the Receiving Party in processing or processing the Producing Party's Protected Information.

D. Inadvertent or unintentional production of documents or things containing Protected Information which are not designated as one or more of the three categories of Protected Information at the time of production shall not be deemed a waiver in whole or in part of a claim for confidential treatment. With respect to such documents, the Producing Party shall immediately upon discovery notify the other Parties of the error in writing and provide replacement pages bearing the appropriate confidentiality legend. In the event of any disclosure of Protected Information other than in a manner authorized by this Protective Order, including any unintentional or inadvertent disclosure, counsel for the Party responsible for the disclosure shall immediately notify opposing counsel of all of the pertinent facts, and make every effort to further prevent unauthorized disclosure including, retrieving all copies of the Protected Information from the recipient(s) thereof, and securing the agreement of the recipients not to further disseminate the Protected Information in any form. Compliance with the foregoing shall not prevent the Producing Party from seeking further relief from the Court.

E. Testifying experts shall not be subject to discovery of any draft of their reports in this case and such draft reports, notes, outlines, or any other writings leading up to an issued report(s) in this litigation are exempt from discovery. In addition, all communications between

counsel for a Party and that Party's testifying expert, and all materials generated by a testifying expert with respect to that person's work, are exempt from discovery unless they relate to the expert's compensation or identify facts, data or assumptions relied upon by the expert in forming any opinions in this litigation and such information is not already disclosed in the expert's report.

F. The United States District Court for the District of Massachusetts is responsible for the interpretation and enforcement of this Protective Order. After termination of this litigation, the provisions of this Protective Order shall continue to be binding except with respect to those documents and information that become a matter of public record. This Court retains and shall have continuing jurisdiction over the parties and recipients of the Protected Information for enforcement of the provisions of this Protective Order following termination of this litigation. All disputes concerning Protected Information produced under the protection of this Protective Order shall be resolved by the United States District Court for the District of Massachusetts.

G. Nothing in this Protective Order shall preclude or impede outside litigation counsel of record's ability to communicate with or advise their client in connection with this litigation only based on such counsel's review and evaluation of Protected Information, provided however, that such communications or advice shall not disclose or reveal the substance or content of any Protected Information other than as permitted under this Protective Order.

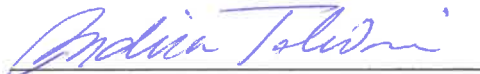
H. Each of the Parties agrees to be bound by the terms of this Protective Order as of the date counsel for such Party executes this Protective Order, even if prior to entry of this order by the Court.

## **27. Termination**

The termination of this Action shall not automatically terminate the effectiveness of this Order and persons subject to this Order shall be bound by the confidentiality obligations of this

Order until the Producing Party agrees otherwise in writing or this Court (or any other court or competent jurisdiction) orders otherwise.

Dated: April 6, 2020



Talwani, I  
U.S. District Court Judge

**EXHIBIT A**

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

TIMMINS SOFTWARE CORPORATION d/b/a  
MITREND

Plaintiff,

v.

EMC CORPORATION, DELL TECHNOLOGIES  
INC., and DELL INC.

Defendants.

C.A. No. 1:19-12053-IT

**JURY TRIAL DEMANDED**

**AGREEMENT TO BE BOUND BY ORDER**

I, \_\_\_\_\_, declare that:

1. My address is \_\_\_\_\_ and the name and address of my  
present employer is \_\_\_\_\_.

2. My present occupation or job description is \_\_\_\_\_.

3. In addition to other job functions, I am working as a consultant  
to \_\_\_\_\_.

4. My relationship to \_\_\_\_\_ is  
\_\_\_\_\_.

5. I have received a copy of the Confidentiality Stipulation and Protective Order (the  
“Order”) in this action.

6. I have carefully read and understand the provisions of the Order, agree to be  
bound by them, and specifically agree I will not use or disclose to anyone any of the contents of

any Protected Information received under the protection of the Protection Order in violation thereof.

7. I understand that I am to retain all copies of any of the materials that I receive that have been so designated as “CONFIDENTIAL,” “HIGHLY CONFIDENTIAL” and/or “HIGHLY CONFIDENTIAL – SOURCE CODE” in a container, cabinet, drawer, room, or other safe place in a manner consistent with the Order and that all copies are to remain in my custody until I have completed my assigned or legal duties. I will return or destroy all Protected Information that comes into my possession or that I have prepared relating thereto, to counsel for the party by whom I am retained. I acknowledge that such return or the subsequent destruction of such materials shall not relieve me from any of the continuing obligations imposed upon me by the Order.

8. I consent to the exercise of personal jurisdiction by this Court in connection with this Declaration and my obligations under the Order.

9. I declare under penalty of perjury that the foregoing is true and correct.

Executed this \_\_\_\_ day of \_\_\_\_\_, 20\_\_ at \_\_\_\_\_  
in the State of \_\_\_\_\_.

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Print Name)